

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR AN ANTICIPATORY SEARCH WARRANT**

I, Terrance L. Taylor, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been so employed since March 2012. I am currently assigned to the Office of the Resident Agent in Charge HSI Charleston, West Virginia. I have experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

2. Prior to my employment with HSI, I was a Police Officer for two years in Huntington, West Virginia, a Special Agent with the United States Department of State-Bureau of Diplomatic Security for six years, a Special Agent with the Naval Criminal Investigative Service for two years, and a Special Agent with the United States Department of State-Office of Inspector General for

two years. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Center ("FLETC") and a graduate of the West Virginia State Police Academy. I graduated from the Criminal Investigator Training Program in 2002, and the Immigration and Customs Enforcement Special Agent Training Program in 2012. As part of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. I have specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18, United States Code, Sections 2251, 2252, 2252A, and 2256.

3. As a Special Agent, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training at the FLETC, Immigration and Customs Enforcement, as well as everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child pornography that occur in the Southern District of West Virginia. I have received training in the areas of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child

pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have obtained search warrants for child pornography offenses, and I have been the case agent or assisted others in numerous investigations involving the sexual exploitation of children. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A(a)(1) (transportation of child pornography), 2252A(a)(2) (receipt or distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), and I am authorized by law to request a search warrant.

4. I make this Affidavit in support of an application for an anticipatory search warrant under Federal Rule of Criminal Procedure 41(b)(1), to search for and seize contraband, evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. §§ 2252A (transportation, receipt, distribution, possession, and access with intent to view child pornography) (collectively, the "Subject Offenses"). Specifically, I seek authorization to search for and seize the items more fully set forth in Attachment B of this Affidavit.

5. These items are believed to be contained in information associated with the Mega LTD ("Mega") account

ALIENATED304@GMAIL.COM,¹ the "Subject Account Information" and the "Subject Account." The Subject Account Information is currently believed to be stored on Mega servers in New Zealand, but is anticipated to be downloaded to computer media in the possession of HSI in the Southern District of West Virginia, as further described in Attachment A.

6. The facts set forth in this Affidavit are based upon my investigation, my training and experience, and information I have received from other law enforcement officers and witnesses. Because I am submitting this Affidavit for the limited purpose of obtaining a search warrant, I have not included each and every fact I know about this investigation. Instead, I have set forth only the facts that I believe are sufficient to establish probable cause that contraband, evidence, fruits, and/or instrumentalities of violations of the Subject Offenses will be located in the Subject Account Information at the time the warrant is executed.

II. BACKGROUND ON MEGA

7. In my training, experience, and research, I have learned that Mega is a company that provides file-hosting and communications services to the public through the website Mega.nz.

¹As described in paragraph eight, a Mega username takes the form of the full email address submitted by the user to create the account.

Mega is headquartered at Level 21, Huawei Centre, 120 Albert Street, Auckland, New Zealand. On information and belief, Mega's computer servers are located in New Zealand, and Mega does not have offices or employees in the United States.

8. A Mega user can sign up for an account with a valid email address, which becomes the user's Mega username. Mega provides users with a certain amount of free data storage; if a user wants more storage, the user can pay for it. Users can access Mega through the Internet from most major devices and platforms from anywhere in the world. For example, a user may take a photo with their cell phone, upload that photo to Mega, and then delete the photo from their cell phone. The photo then resides on Mega's servers. The user can then access their Mega account from a different device, such as a desktop computer, and download the photo to that computer.

9. A Mega user can designate a special folder (or folders) on their computer, which Mega synchronizes with the user's account. As a result, that same folder, with the same contents, will appear on both the user's computer and their Mega account. Files placed in that folder are accessible through Mega's website, as well as its mobile-phone applications.

10. In addition, Mega users can share files with other people by sending web links, which give access to the particular shared files.

11. Another feature of Mega is "MegaChat," which allows users to exchange messages and have audio, video, and group chats.

12. According to Mega, data associated with a Mega account is stored on Mega's servers in an encrypted format. Data is also transmitted in an encrypted format between Mega's servers and users' devices. Messages between Mega users are also transmitted in an encrypted format within Mega's secure server network. Because data is encrypted at all steps, the risk of files or messages being intercepted is minimal.

13. Mega's server architecture means that data is encrypted in a way that makes it generally inaccessible to Mega. Data is encrypted on the client side using an encryption key to which Mega does not have access. This means that, barring exceptional circumstances, Mega does not have the technical ability to decrypt user's files or messages and, as a result, Mega is unable to provide data in a usable format to third parties. Mega also is unable to conduct data recovery. If a user forgets their password, Mega cannot recover the user's data.

14. Due to its encryption, MEGA has become a popular cloud-based storage repository and/or location to distribute Child

Sexual Abuse Material (CSAM). Since MEGA does not restrict the same IP address from creating more than one MEGA account, persons involved in the receipt, collection, and distribution of CSAM often have multiple MEGA accounts.

15. As explained herein, the Subject Account Information may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This information can indicate who used or controlled the Subject Account. For example, communications, contacts lists, and files sent or uploaded (and the metadata associated with the foregoing, such as date and time) may indicate who used or controlled the Subject Account at a relevant time. The information may also reveal the identity of other victims and the underlying time frames in which they were victimized (e.g., folders with victim data and the metadata associated with file transfers). Additionally, stored electronic data may provide relevant insight into the Subject Account owner's state of mind as it relates to the offenses under investigation. For example, information in the Subject Account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime) or consciousness of guilt

(e.g., deleting communications in an effort to conceal them from law enforcement).

III. PROBABLE CAUSE

16. On or about January 16, 2023, Snapchat submitted CyberTipline Report #152857798 to the National Center for Missing and Exploited Children ("NCMEC"). The incident type was identified as apparent child pornography, and the incident time was listed as: January 15, 2023, at 18:05:59 UTC.

17. Snapchat uploaded two files in connection with the report, each containing apparent child pornography. Snapchat reported that the files at issue were uploaded by Snapchat username "alienated5555," email address ALIENATED2323@GMAIL.COM, date of birth 07-xx-19xx, and IP address 47.213.82.125.

18. On or about January 16, 2023, your Affiant reviewed the two files associated to the CyberTip and found those to contain the following: (1) an image depicting a white, nude, prepubescent female approximately 3-5 years old; the female performed fellatio on a white, adult male; and (2) an image depicting a white, nude, prepubescent female lying on her back; the image focused on her naked vagina and semen was observed on her leg and vagina.

19. Further investigation revealed that the IP address provided in the Cybertip, 47.213.82.125, resolved to Suddenlink

Communications. The account listed the subscriber as Phillip Mace with an account address of 121 Hastings Drive, Belle, WV 25015, and a phone number of 304-949-3276.

20. Law enforcement was able to link both Phillip Mace and Toni Mace to the residence using driver's licenses databases. Law enforcement was able to determine that Phillip Mace and Toni Mace were married.

21. On March 7, 2023, a federal search warrant was obtained to search the Belle residence belonging to Phillip and Toni Mace. The search warrant was executed on March 16, 2023.

22. During the search warrant execution Toni Mace agreed to speak with your Affiant. Your Affiant advised Toni Mace of the federal search warrant regarding the search and seizure of her electronic devices to include cellphones, computers, and external storage devices. Toni Mace stated she understood and advised that her husband, Phillip Mace, was currently in the hospital for medical issues. No other individuals live at the residence.

23. Toni and Phillip Mace's son, Phillip Mace II, died due to drug dependence issues in October 2022. Toni Mace advised that their son lived down the street at 125 Hastings Drive, Belle, West Virginia ("125 Hastings Drive residence"). Phillip and Toni Mace own the residence and allowed their son and his fiancé, Cynthia Ellis ("Ellis"), to live there. After her son's death, Ellis

continued to reside at the 125 Hastings Drive residence.

24. Toni Mace stated she and her husband use Suddenlink/Optimum as their internet service provider. They have a Wi-Fi router that is password protected. She further advised that the Wi-Fi could be accessed from both the 121 Hastings Drive residence, and the 125 Hastings Drive residence. Toni Mace further advised that she was aware that her deceased son accessed the internet using her Suddenlink/Optimum Wi-Fi and password at the 125 Hastings Drive residence. When Toni Mace changed the locks on the 125 Hastings Drive residence recently, she found her Wi-Fi router name and password taped to the window within the 125 Hastings Drive residence.

25. Toni Mace advised that since her son's death in October 2022, a man she knew as J.D. CARROLL lived with Ellis at the 125 Hastings Drive residence.

26. Through further investigation, law enforcement was able to link the man Toni Mace knew as J.D. CARROLL to Jerry Dewayne CARROLL ("CARROLL"). CARROLL was issued a West Virginia driver's license (#F097645), with a date of birth as July xx, 19xx. This date of birth matches the date of birth Snapchat provided for user alienated5555, as indicated in the Cypertip.

27. Law enforcement analysts were further able to link the email address ALIENATED2323@GMAIL.COM from the Cybertip to

CARROLL.

28. On April 7, 2023, a federal search warrant was obtained to search the person of CARROLL. The search warrant was executed on April 10, 2023. During the search warrant execution, one electronic device was seized from CARROLL's person, specifically a One Plus cellphone.

29. The One Plus cellphone was subsequently forensically reviewed. The phone contained 1,400 images of child pornography. Furthermore, the cellphone revealed evidence of the use of Mega. Law enforcement was further able to determine that the Mega account utilized by CARROLL had the username ALIENATED2323@GMAIL.COM. Further, law enforcement found evidence on the One Plus cellphone that this email address had been accessed on the cellphone.

30. On or about May 18, 2023, law enforcement sent a request to Mega for data associated with the Mega account ALIENATED2323@GMAIL.COM to be preserved for 90 days.

31. Mega further provided law enforcement with subscriber and other non-content information regarding the Mega account for ALIENATED2323@GMAIL.COM. This information indicated that the account had been accessed from IP address 47.213.82.125, which is the same IP address identified in the Snapchat Cybertip.

32. Law enforcement also identified a password associated to the Mega account ALIENATED2323@GMAIL.COM on the One Plus cellphone.

33. On June 6, 2023, a federal search warrant was obtained to search the Mega account ALIENATED2323@GMAIL.COM associated to CARROLL. The search warrant was executed on June 9, 2023. The forensic review of the aforementioned Mega account contained 82 child pornography videos.

34. Subsequent investigation identified the minor child victim associated to the Snapchat Cybertip. The photograph, as described in Paragraph 18, depicted a 3-5 year old female performing fellatio on an unknown adult male. The minor victim was identified by her mother. The minor victim's mother also stated that CARROLL was her cousin and had access to the minor victim in the summer of 2020.

35. Law enforcement identified an additional Mega account utilized by CARROLL that had the username ALIENATED304@GMAIL.COM. Further, law enforcement found evidence on the One Plus cellphone that this email address had been accessed on the cellphone. Law enforcement also recovered the password for the account.

36. On or about February 14, 2024, law enforcement sent a request to Mega for data associated with the Mega account ALIENATED304@GMAIL.COM to be preserved for 90 days.

37. Mega further provided law enforcement with subscriber and other non-content information regarding the Mega account for ALIENATED304@GMAIL.COM. This information indicated that the account had been accessed from IP address 47.213.82.125, which is the same IP address identified in the Snapchat Cybertip.

38. The information in the Subject Account is currently believed to be stored on Mega servers located in New Zealand. It is my understanding that the Fourth Amendment's warrant requirement generally does not apply to locations outside the territorial jurisdiction of the United States, see United States v. Stokes, 726 F.3d 880, 890-93 (7th Cir. 2013), and that a warrant issued under Federal Rule of Criminal Procedure 41 would not authorize the search of a server located in New Zealand under these circumstances. See also United States v. Verdugo-Urquidez, 494 U.S. 259, 274 (1990) (describing a warrant issued by a United States magistrate judge as "a dead letter outside the United States"). Therefore, I seek this warrant out of an abundance of caution, to be certain that an examination of information from the Subject Account (i.e., the Subject Account Information) downloaded to computer media in the possession of HSI in the Southern District of West Virginia will comply with the Fourth Amendment and other applicable laws.

IV. CONDITION REQUIRED PRIOR TO EXECUTION

39. As noted above, the forensic review of the electronic device seized from CARROLL identified the username and password for the Subject Account. Upon information and belief, the information contained in the Subject Account is believed to be located on Mega servers in New Zealand.

40. HSI plans on accessing the Subject Account using the credentials identified in the forensic review of CARROLL's electronic device; if such access is successful, HSI intends to use Mega's data transfer tools to download the account's information onto computer media in the possession of HSI, located in the Southern District of West Virginia. The downloaded information (i.e., the Subject Account Information) may include, but is not limited to, files, communications, and contact lists associated with the Subject Account.

41. I am seeking permission to search the Subject Account Information following the triggering event of the download of said information by HSI into the Southern District of West Virginia, as described in Attachment A, and to seize the items and information described in Attachment B.

42. Manner of Execution. Because this warrant seeks permission only to examine information on computer media in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently,

your Affiant submits there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

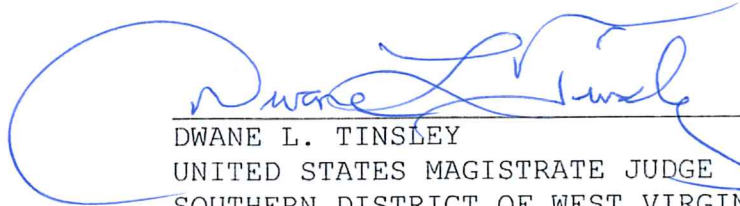
V. CONCLUSION

43. Based on the information described above, your Affiant respectfully submits there is probable cause to believe that contraband, evidence, fruits, and/or instrumentalities of violations of the Subject Offenses, specifically those items more fully set forth in Attachment B, are currently located in the Subject Account, and will be located in the Subject Account Information in the Southern District of West Virginia at the time the warrant is executed.



TERRANCE L. TAYLOR
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this 21st day of February, 2024.



DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA